JOURNAL OF COMBINATORIAL THEORY, Series A 35, 67–78 (1983)

The Existence and Nonexistence of Perfect Addition Sets

CLEMENT W. H. LAM*

Department of Computer Science, Concordia University, Montreal, Canada

AND

S. L. MA AND M. K. SIU

Department of Mathematics, University of Hong Kong

Communicated by the Managing Editors

Received January 20, 1982

A (v, k, λ, μ)-perfect addition set is a subset A of $\mathbb{Z}/v\mathbb{Z}$ with k elements such that the expression $a_i + a_j$, for $a_i \neq a_j$ in A, represents 0 exactly μ times and each nonzero element exactly λ times. Several infinite classes of such sets using quadratic residues of primes, a few isolated examples using cubic residues, and a construction in certain cases when v is twice an odd integer, are given. There is an efficient method, based on the Chinese remainder theorem, which decides the existence or nonexistence of a perfect addition set. Some further results on nonexistence are given. In particular, two previously unsolved cases of Isbell (*Discrete Math.* 24 (1978), 13–18) are settled. The article ends with a list of nontrivial perfect addition sets with $k \leqslant 20$.

1. INTRODUCTION

A (v, k, λ, μ)-*perfect addition set* is a subset A of $\mathbb{Z}/v\mathbb{Z}$ with k elements such that the expression $a_i + a_j$, for $a_i \neq a_j$ in A, represents 0 exactly μ times and each nonzero element exactly λ times.

This definition of a perfect addition set is a generalization of the definition given by Isbell [2] which requires $\mu = 0$. It is different from the "addition set" as defined by Lam [3].

In Section 2, we list several simple results on perfect addition sets. In Section 3, we give several examples of perfect addition sets. In particular, we

* This paper was written while Dr. Lam was visiting the University of Hong Kong.

0097-3165/83 $3.00

establish several infinite classes arising from quadratic residues of primes and a few isolated examples from cubic residues. We also have a construction in certain cases when v is twice an odd integer, In Section 4, we present an efficient method, based on the Chinese remainder theorem, which can decide the existence or nonexistence of a perfect addition set. In Section 5, we prove several nonexistence results. In particular, we show that the two unsolved cases in Isbell [2] do not exist. In Section 6, a list of nontrivial perfect addition sets with $k \leqslant 20$ is given.

2. General Results

The parameters of a perfect addition set satisfy some simple relations.

Proposition 2.1. *The parameters of a perfect addition set satisfy*:

(i) $k^2 - k = \mu + (v-1)\lambda$,

(ii) *both* λ *and* μ *are even*,

(iii) $0 \leqslant \lambda \leqslant k$, *and*

(iv) $0 \leqslant \mu \leqslant k$.

Proof. The $k^2 - k$ expressions $a_i + a_j$, where $a_i \neq a_j$ in A, represent 0 exactly μ times and each of the other $v-1$ nonzero values exactly λ times. Thus, we have (i). Relation (ii) holds because $a_i + a_j = a_j + a_i$. It is clear that both λ and μ are greater than or equal to 0. The facts that $\lambda \leqslant k$ and $\mu \leqslant k$ hold because once a_i is fixed, the expression $a_i + a_j$ can represent a given value at most once. Q.E.D.

The *Hall polynomial* of a set A of residues modulo v is the polynomial

$$\theta(x) = x^{a_1} + \cdots + x^{a_k}, \tag{2.1}$$

where $a_i \in A$.

In terms of polynomials, the property of a perfect addition set gives

Theorem 2.2. *A set* A *of* k *distinct residues modulo* v *is a* (v, k, λ, μ)-*perfect addition set if and only if its Hall polynomial satisfies*

$$\theta(x)^2 - \theta(x^2) \equiv (\mu - \lambda) + \lambda T(x) \qquad (\text{mod } x^v - 1), \tag{2.2}$$

where $T(x) = 1 + x + \cdots + x^{v-1}$.

3. Examples

It is easy to write a list of trivial perfect addition sets.

Proposition 3.1. *The following sets are perfect addition sets:*

(i) $A = \varnothing$ *is a* $(v, 0, 0, 0)$*-perfect addition set,*

(ii) $A = \{a\}$ *for any residue* a *is a* $(v, 1, 0, 0)$*-perfect addition set,*

(iii) $A = \{a, v - a\}$ *for any residue* $a \not\equiv v - a \pmod{v}$ *is a* $(v, 2, 0, 2)$*-perfect addition set,*

(iv) $A = \{0, 1, \ldots, v - 1\}$, *for* v *odd, is a* $(v, v, v - 1, v - 1)$*-perfect addition set,*

(v) $A = \{1, \ldots, v - 1\}$, *for* v *odd, is a* $(v, v - 1, v - 3, v - 1)$*-perfect addition set,*

(vi) $A = \{0, 1\}$ *is a* $(2, 2, 2, 0)$*-perfect addition set, and*

(vii) $A = \{0, 1, 2\}$ *is a* $(4, 3, 2, 0)$*-perfect addition set.*

A perfect addition set, where $k \leqslant 2$ or $k \geqslant v - 1$, is said to be *trivial.* It is simple to show that the only trivial perfect addition sets are the ones listed in Proposition 3.1. A perfect addition set, where $2 < k < v - 1$ is said to be *nontrivial.*

From a (v, k, λ, μ)-perfect addition set, we can sometimes construct another.

Construction 3.2. *If a* (v, k, λ, μ)*-perfect addition set exists with* $\lambda = 2k + 1 - v$, *then a* $(2v, v + k, 2k, \mu')$*-perfect addition set exists, where* $\mu' = (v - k)^2 - (v - k)$.

Proof. Let A be the (v, k, λ, μ)-perfect addition set. The new perfect addition set A' consists of all the odd numbers $1, 3, \ldots, 2v - 1$ and the numbers $2a_i$, where $a_i \in A$. It is easy to verify that the odd values are represented $2k$ times by the form $x + y$ with $x \neq y$ in A'. The nonzero even values are represented $(v - 1) + \lambda$ times. Thus, if $\lambda = 2k + 1 - v$, then all nonzero values are represented $2k$ times. It is then easy to verify that the parameters are the one as shown. Q.E.D.

Example 3.3. Starting from the trivial $(5, 2, 0, 2)$-perfect addition set $\{1, 4\}$, we get the nontrivial $(10, 7, 4, 6)$-perfect addition set $\{1, 3, 5, 7, 9, 2, 8\}$.

Cyclotomy was first used by Lehmer [5] to construct difference sets. For a detailed treatment of cyclotomy, please see Baumert [1] or Storer [6].

Let $p = Nf + 1$ be an odd prime and let α be a fixed primitive root of p. The index class l with respect to α is

$$C_l = \{\alpha^{Ni+l} \mid i = 0, 1, \ldots, f-1\}. \tag{3.1}$$

The *cyclotomic number* $(l, m)_N$ is the number of solution pairs (x, y) to the congruence

$$x + 1 \equiv y \pmod{p} \tag{3.2}$$

with x in the index class C_l and y in the index class C_m. Based on the notation of Lam [4], we let $\rho_j(x)$ denote the Hall polynomial of the index class C_j, that is, $\rho_j(x) = \sum_{x \in C_j} x^r$. We let

$$\theta(x) = r + \sum_{j=0}^{N-1} b_j \rho_j(x), \tag{3.3}$$

where the r and b_j's are 0 or 1.

LEMMA 3.4. *Let $\theta(x)$ be given by* (3.3). *Then*:

(i) $$\theta(x^2) \equiv r + \sum_{s=0}^{N-1} b_{s-\gamma} \rho_s(x) \pmod{x^p - 1},$$

where the residue 2 *is in the index class γ and the subscript $s - \gamma$ is reduced modulo N, and*

(ii) $$\theta(x)^2 \equiv \text{constant} + \sum_{s=0}^{N-1} J_s \rho_s(x) \pmod{x^p - 1},$$

where

$$J_s = 2rb_s + \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} b_i b_j (i-j, s-j)_N. \tag{3.4}$$

Proof. Equation (i) follows from the fact that if $x \in C_{j-\gamma}$, then $2x \in C_\gamma$. Equation (ii) follows from the fact that

$$\rho_i(x)\rho_j(x) \equiv \text{constant} + \sum_{s=0}^{N-1} (i-j, s-j)_N \rho_s(x) \pmod{x^p - 1}. \tag{3.5}$$

This is because the number of solutions to $x + y \equiv z \pmod{p}$ with $x \in C_i$, $y \in C_j$, and $z \in C_s$ is the same as the number of solutions to $xy^{-1} + 1 \equiv zy^{-1} \pmod{p}$ which is $(i-j, s-j)_N$. Q.E.D.

THEOREM 3.5. *Suppose $\theta(x)$ is in the form* (3.3) *and J_s is defined by* (3.4). *Then $\theta(x)$ is the Hall polynomial of a (p, k, λ, μ)-perfect addition set if and only if $J_s - b_{s-\gamma}$ is λ for all s.*

Proof. The proof follows from Theorem 2.2 and Lemma 3.4. Q.E.D.

COROLLARY 3.6. *Let γ be the index class to which 2 belongs. A necessary and sufficient condition that the* Nth *power residues of a prime $v = Nf + 1$ form a (v, k, λ, μ)-perfect addition set is that*

$$(0, N-\gamma)_N - 1 = \lambda \qquad \text{and} \qquad (0, i)_N = \lambda \qquad \text{for} \quad i \neq N - \gamma.$$

A necessary and sufficient condition that the Nth *power residues and zero for a prime $v = Nf + 1$ form a (v, k, λ, μ)-perfect addition set is that*

$$(0, 0)_N + 1 = (0, i)_N = \lambda \qquad \text{for} \quad i = 1, \ldots, f-1 \quad \text{when} \quad \gamma = 0$$

and

$$(0, 0)_N + 2 = (0, N-\gamma)_N - 1 = \lambda \qquad \text{and} \qquad (0, i)_N = \lambda \qquad \text{for} \quad i \neq 0$$

or $N - \gamma$ when $\gamma \neq 0$.

CONSTRUCTION 3.7. *The quadratic residues of a prime v form a (v, k, λ, μ)-perfect addition set in the following two cases*:

(i) $(v, k, \lambda, \mu) = (8t + 3, 4t + 1, 2t, 0)$, *and*

(ii) $(v, k, \lambda, \mu) = (8t + 5, 4t + 2, 2t, 4t + 2)$.

The quadratic residues and zero of a prime v form a (v, k, λ, μ)-perfect addition set in the following two cases:

(iii) $(v, k, \lambda, \mu) = (8t + 1, 4t + 1, 2t, 4t)$, *and*

(iv) $(v, k, \lambda, \mu) = (8t + 7, 4t + 4, 2t + 2, 0)$.

Proof. The cyclotomic numbers for $N = 2$ can be found in Storer [6, p. 30]. In particular, for f even, $(0, 0)_2 = (f - 2)/2$ and $(0, 1)_2 = f/2$. For f odd, $(0, 0)_2 = (f - 1)/2$ and $(0, 1)_2 = (f + 1)/2$. The residue 2 is in class C_0 when $v \equiv 1$ or 7 (mod 8) and is in class C_1, otherwise. The proof is now a simple application of Corollary 3.6. Q.E.D.

Cases (i) and (iv) were already reported in Isbell [2, Theorem 1.1]. It should be noted that there are no other perfect addition sets arising from quadratic residues.

The following examples are constructed from cubic residues.

CONSTRUCTION 3.8. *For $N = 3$, the following sets are perfect addition sets*:

(i) *The cubic residues and zero of* $p = 37$ *forms a* $(37, 13, 4, 12)$*-perfect addition set*;

(ii) *the union of classes* C_0 *and* C_1 *for* $p = 13$ *forms a* $(13, 8, 4, 8)$*-perfect addition set*; *and*

(iii) *the union of classes* C_0 *and* C_1 *with the element* 0 *for* $p = 19$ *forms a* $(19, 13, 8, 12)$*-perfect addition set.*

Proof. The proofs for all three cases are similar and we shall only do case (iii). In this case, $r = b_0 = b_1 = 1$ and $b_2 = 0$. Equation (3.4) implies that

$$J_0 = 2 + (0, 0)_3 + (2, 2)_3 + (1, 0)_3 + (0, 2)_3,$$
$$J_1 = 2 + (0, 1)_3 + (2, 0)_3 + (1, 1)_3 + (0, 0)_3,$$

and

$$J_2 = 0 + (0, 2)_3 + (2, 1)_3 + (1, 2)_3 + (0, 1)_3.$$

By choosing 2 as the primitive root of 19, we have $\gamma = 1$ and the cyclotomic numbers are given in the cyclotomic matrix

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & 1 & 2 \end{array} \\ \begin{bmatrix} 2 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \end{array}.$$

Thus, $J_0 = 8$ and $J_1 = J_2 = 9$. Hence, $J_s - b_{s-\gamma}$ is 8 for all s. Q.E.D.

4. Polynomial Congruences

In this section, we develop an efficient method for finding solutions to the congruence equation

$$\theta(x)^2 - \theta(x^2) \equiv (\mu - \lambda) + \lambda T(x) \qquad \text{mod}(x^v - 1), \tag{4.1}$$

where $\theta(x)$ has nonnegative integral coefficients. It uses the Chinese remainder theorem and is motivated by Baumert [1, pp. 65–68]. Baumert's method is based on the idea that a $\theta(x)$ modulo $x^v - 1$ is uniquely determined by a set of polynomials $\theta_w(x)$ with $w \mid v$, where $\theta(x) \equiv \theta_w(x)$ modulo $f_w(x)$ and $f_w(x)$ is the irreducible polynomial satisfied by the primitive wth roots of unity. If $\theta(x)$ satisfies a congruence equation, then all the $\theta_w(x)$ have to satisfy similar equations. The difficulty with this method is in finding an exhaustive list of candidates for $\theta_w(x)$.

Our idea is to choose a prime p of the form $p = ev + 1$ and consider

applying the Chinese remainder theorem on $\theta(x) \pmod{x^v - 1, p}$. In this case, an exhaustive list of candidates can often be found easily.

We let g be a primitive root modulo p. We let $\omega = g^e$ and we note that ω^i, $i = 0, 1, \ldots, v-1$ are all distinct. Since $(\omega^i)^v \equiv 1 \pmod{p}$ for all j, we have

$$x^v - 1 \equiv \prod_{i=0}^{v-1} (x - \omega^i) \pmod{p}. \tag{4.2}$$

We let $f_i(x) = x - \omega^i$. We further note that $f_i(x)$ divides $f_{2i}(x^2)$ since $f_{2i}(x^2) = (x - \omega^i)(x + \omega^i)$. For each $\theta(x) \pmod{x^v - 1, p}$, we associate a set of residues $\{r_i \equiv \theta(\omega^i) \bmod p\}$ which are the remainder of $\theta(x)$ when divided by $f_i(x)$ modulo p. It is simple to see that $\theta(x) \pmod{x^v - 1, p}$ is uniquely determined by the set of residues $\{r_i\}$ because $\theta(x)$ is a polynomial of degree less than v with coefficients from the field $\mathbb{Z}/p\mathbb{Z}$ and its values on v distinct points $\{\omega^i, i = 0, 1, \ldots, v-1\}$ are known. In fact, $\theta(x)$ can be reconstructed from $\{r_i\}$ by a standard interpolation formula.

Now, we claim

THEOREM 4.1. *A polynomial $\theta(x)$ satisfies*

$$\theta(x)^2 - \theta(x^2) \equiv (\mu - \lambda) + \lambda T(x) \pmod{x^v - 1, p} \tag{4.3}$$

if and only if

$$r_0^2 - r_0 \equiv \mu + \lambda(v-1) \pmod{p}, \tag{4.4}$$

and

$$r_i^2 - r_{2i} \equiv \mu - \lambda \pmod{p} \quad \text{for} \quad i = 1, \ldots, v-1, \tag{4.5}$$

and where the subscript $2i$ is taken modulo v.

Proof. We consider the effect of reducing Eq. (4.3) modulo $f_i(x)$. We first note that the facts $r_{2i} \equiv \theta(x) \pmod{f_{2i}(x), p}$ and $f_i(x)$ divides $f_{2i}(x^2)$ imply that $r_{2i} \equiv \theta(x^2) \pmod{f_i(x), p}$. Thus, the left-hand side is $r_i^2 - r_{2i}$. The right-hand side is $\mu + \lambda(v-1)$ when $i = 0$ and $\mu - \lambda$ when $i \neq 0$. Thus, if $\theta(x)$ satisfies (4.3), then its residues satisfy (4.4) and (4.5). Conversely, the Chines remainder theorem implies that if the r_i's satisfy (4.4) and (4.5), then $\theta(x)$ satisfies (4.3). Q.E.D.

As an example, let us consider finding a $(7, 4, 2, 0)$-perfect addition set. We choose $p = 29$, with 2 as the primitive root and $\omega = 16$. Since $r_0 = \theta(1) = k$, r_0 is 4. There are 29 possibilities for r_1. Once r_1 is choosen, we can find r_2 using (4.5). From r_2 we get r_4. From r_4 we get r_1 which must be the same as the one we started with. Similarly, from r_3 we get r_6, r_5, and then r_3 again.

The only possibilities are $r_1 = r_2 = r_4 = 8$ or 22 and $r_3 = r_6 = r_5 = 8$ or 22. From the Lagrange interpolation formula, we derive that

$$\theta(x) = \frac{1}{v} \sum_{i=0}^{v-1} \frac{r_i \omega^i (x^v - 1)}{x - \omega^i} \qquad (\mathrm{mod}\ x^v - 1, p). \tag{4.6}$$

In particular, the constant term of $\theta(x)$ is given by $v^{-1} \sum_{i=0}^{v-1} r_i$. If $\theta(x)$ has $(0, 1)$ coefficients, then $\sum_{i=0}^{v-1} r_i$ is 0 or v. In our case, if $r_1 = 8$, then $r_3 = 22$ or vice versa. Choosing $r_1 = r_2 = r_4 = 8$ and $r_3 = r_5 = r_6 = 22$, we get $\theta(x) = 1 + x + x^2 + x^4$. The other choice gives $\theta(x) = 1 + x^3 + x^5 + x^6$.

We can use this method to show that the unsolved cases of Isbell [2] do not exist. For example, for $(v, k, \lambda, \mu) = (61, 16, 4, 0)$, we use $p = 367$. The only possible choices for r_1 are 63 or 303. Once r_1 is fixed, r_2 to r_{10} are all determined. They both give rise to a $\theta(x)$ with a constant term of 84.

5. Nonexistence Results

THEOREM 5.1. *If a (v, k, λ, μ)-perfect addition set exists, then* $v \geqslant 2k - \mu - 2$.

Proof. Since the value 0 is represented μ times, the perfect addition set A must contain $\mu/2$ pairs of the form $(a, -a)$ with $a \neq -a$. If x is one of the remaining $k - \mu$ elements of A and $x \neq -x$, then $-x \notin A$. There can be at most two elements such that $x = -x$. Thus, by counting the elements, we have $2(k - \mu - 2) + 2 + \mu \leqslant v$ or $2k - \mu - 2 \leqslant v$. Q.E.D.

Theorem 5.1 is similar to [2, Eq. (2)]. Theorem 5.2 is similar to [2, Theorem 1.3].

THEOREM 5.2. *If a (v, k, λ, μ)- perfect addition set exists with v even, then $k + \mu - \lambda$ is a square.*

Proof. Substituting $x = -1$ in (2.2), we have

$$\theta(-1)^2 = \theta(1) + (\mu - \lambda) = k + \mu - \lambda. \qquad \text{Q.E.D.}$$

Theorem 5.3 is similar to [2, Theorem 1.4].

THEOREM 5.3. *If there is a (v, k, λ, μ)-perfect addition set and 4 divides v, then either $|\mu - \lambda + \sqrt{k + \mu - \lambda}|$ or $|\mu - \lambda - \sqrt{k + \mu - \lambda}|$ is a square.*

Proof. Substituting $x = i$ in (2.2), we have $\theta(i)^2 = \theta(-1) + \mu - \lambda = \mu - \lambda \pm \sqrt{k + \mu - \lambda}$. However, $\theta(i) = \alpha + \beta i$ for some integers α and β. Thus, $\theta(i)^2 = \alpha^2 - \beta^2 + 2\alpha\beta i$. Equating the imaginary parts, we have either $\alpha = 0$ or $\beta = 0$. Hence, $\theta(i)^2$ is either a square or minus a square. Q.E.D.

THEOREM 5.4. *If there is a* (v, k, λ, μ)*-perfect addition set and* 3 *divides* v*, then either* $1 + 4(\mu - \lambda)$ *is a square or* $k \equiv 1 \pmod 3$ *and* $1 - 4(\mu - \lambda)/3$ *is a square.*

Proof. We let $cx^2 + bx + a$ be the residue of $\theta(x)$ modulo $x^3 - 1$. We also let $t = v/3$. Equation (2.2), when taken modulo $x^3 - 1$ implies

$$2ac + b^2 - b = \lambda t, \tag{5.1}$$

$$2ab + c^2 - c = \lambda t, \tag{5.2}$$

and

$$2bc + a^2 - a = \lambda(t - 1) + \mu. \tag{5.3}$$

From (5.1) and (5.2), we have $2a(b - c) + (b - c) = (b - c)(b + c)$, which implies either $b = c$ or $2a + 1 = b + c$.

If $b = c$, then from (5.1) and (5.3) we have

$$(a - b)^2 - (a - b) - (\mu - \lambda) = 0. \tag{5.4}$$

Since $a - b$ is an integer, the discriminant of (5.4) is a square. Therefore, $1 + 4(\mu - \lambda)$ is a square.

If $2a + 1 = b + c$, then $k = a + b + c = 3a + 1$. Moreover, substituting $c = 2a + 1 - b$ into (5.1), we have

$$b^2 - (1 + 2a)b + 2a(2a + 1) - \lambda t = 0. \tag{5.5}$$

Again, since b is an integer, the discriminant $1 - 4ak + 4\lambda t$ is a square. Using Proposition 2.1(i) we have $k(k - 1) = 3t\lambda + (\mu - \lambda)$ which implies that $ak = t\lambda + (\mu - \lambda)/3$. Thus, $1 - 4(\mu - \lambda)/3$ is a square. Q.E.D.

Theorem 5.4 is similar to the second part of [2, Theorem 1.3]. For example, the case $(v, k, \lambda, \mu) = (27, 13, 6, 0)$ is eliminated by the previous theorem.

Suppose $v = 2^s w$, where w is odd. We let ξ denote a primitive vth root of unity. The next nonexistence result requires a bound on $|\theta(\xi^j)|$. We let L be $(1 + \sqrt{1 + 4|\mu - \lambda|})/2$.

LEMMA 5.5. *If* $\theta(x)$ *satisfies* (2.2) *and if* $w \nmid j$, $j < v$, *then* $|\theta(\xi^j)| \leqslant L$.

Proof. We let $g(x) = x^2 - (\mu - \lambda)$. Therefore, $|g(x)| \geqslant |x|^2 - |\mu - \lambda|$ for any complex value x. If $|x| > L$, then $|x|^2 - |x| - |\mu - \lambda| > 0$. Hence, we have $|g(x)| > |x|$ if $|x| > L$. Since $2^t j \not\equiv 0 \pmod v$ for all t, there exist two positive integers r and s such that $2^r j \equiv 2^s j \pmod v$ and $r < s$. Clearly,

$\xi^{2^r j} = \xi^{2^s j}$ and $\theta(\xi^{2^r j}) = \theta(\xi^{2^s j})$. Since $|\theta(\xi^j)| > L$ and $\xi^j \neq 1$, we use Eq. (2.2) to conclude that $|\theta(\xi^{2j})| = |g(\theta(\xi^j))| > |\theta(\xi^j)| > L$. Repeated applications of Eq. (2.2) gives $|\theta(\xi^{2^s j})| > |\theta(\xi^{2^r j})| > L$. Thus, it contradicts $\theta(\xi^{2^s j}) = \theta(\xi^{2^r j})$.

Q.E.D.

We next bound the size of those $\theta(\xi^j)$ for which $w \mid j$, $0 < j < v$; that is, there exists an $i > 0$ such that $2^i j \equiv 0 \pmod v$. We define $h_0 = \sqrt{k + \mu - \lambda}$. If $|\mu - \lambda| + h_0$ is a square, then we define $h_1 = \sqrt{|\mu - \lambda| + h_0}$; otherwise, we define $h_1 = \sqrt{|(\mu - \lambda) - h_0|}$. For $i > 1$, we define $h_i = \sqrt{|\mu - \lambda| + h_{i-1}}$. In these definitions, we always use the positive square root.

LEMMA 5.6. *If $\theta(x)$ satisfies (2.2) and $i > 0$ is the smallest integer such that $2^i j \equiv 0 \pmod v$, then $|\theta(\xi^j)| \leqslant h_{i-1}$.*

Proof. For $i = 1$, we have $|\theta(\xi^j)| = |\theta(-1)| = h_0$. For $i = 2$, we have $|\theta(\xi^j)| = |\theta(\pm i)| \leqslant h_1$, by the proof of Theorem 5.3. Since $\theta(\xi^j)^2 = \theta(\xi^{2j}) + (\mu - \lambda)$, we have

$$|\theta(\xi^j)| \leqslant \sqrt{|\theta(\xi^{2j})| + |\mu - \lambda|} \leqslant \sqrt{h_{i-2} + |\mu - \lambda|} = h_{i-1}. \qquad \text{Q.E.D.}$$

THEOREM 5.7. *Suppose $v = 2^s w$, where w is odd. Then $L^2(v - 2^s) + \sum_{i=1}^{s} 2^{i-1} h_{i-1}^2 \geqslant vk - k^2$, where $L = (1 + \sqrt{1 + 4|\mu - \lambda|})/2$ and h_i is as defined above.*

Proof. We let

$$\theta(x)\,\theta(x^{-1}) \equiv a_0 + a_1 x + \cdots + a_{v-1} x^{v-1} \pmod{x^v - 1}. \tag{5.6}$$

Again, the polynomial on the right-hand side of (5.6) is uniquely determined once its values on the v points ξ^j, $j = 0, 1, \ldots, v - 1$ are known. In particular, the coefficient a_0 is given by

$$a_0 = \frac{1}{v} \sum_{j=0}^{v-1} (\theta(\xi^j)\,\theta(\xi^{-j})) = \frac{1}{v} \sum_{j=0}^{v-1} |\theta(\xi^j)|^2. \tag{5.7}$$

On the other hand, since $\theta(x)$ has $(0, 1)$ coefficients, $a_0 = k$. Together with the fact $\theta(\xi^0) = k$, we have

$$\sum_{j=1}^{v-1} |\theta(\xi^j)|^2 = vk - k^2.$$

There are $v - 2^s$ j's $(1 \leqslant j \leqslant v - 1)$ such that $w \nmid j$. For the remaining j's, which are $w, 2w, \ldots, (2^s - 1)w$, we count that for a given i $(1 \leqslant i \leqslant s)$, there are 2^{i-1} of them which satisfy $2^{s-i} w \mid j$ but $2^{s-i+1} w \nmid j$; that is, for which i is

the smallest positive integer such that $2^i j \equiv 0 \pmod{v}$. We apply Lemma 5.5 to the former case and Lemma 5.6 to the latter case to obtain

$$L^2(v-2^s)+\sum_{i=1}^{s} 2^{i-1}h_{i-1}^2 \geqslant vk-k^2. \qquad \text{Q.E.D.} \tag{5.8}$$

Both unsolved cases $(v, k, \lambda, \mu) = (41, 16, 6, 0)$ and $(61, 16, 4, 0)$ of Isbell [2] are eliminated by Theorem 5.7. For both of these cases, v is odd and the left-hand side of inequality (5.8) reduces to $L^2(v-1)$.

6. List of $k \leqslant 20$

Table I gives a list of nontrivial perfect addition sets with $k \leqslant 20$. A computer program was used to generate a list of all parameters for

TABLE I

A List of Nontrivial Perfect Addition Sets for $3 \leqslant k \leqslant 20$

v	k	λ	μ	A	Type[a]
7	4	2	0	0, 1, 2, 4.	Q
6	4	2	2	0, 1, 3, 5.	D
11	5	2	0	1, 3, 4, 5 , 9.	Q
9	5	2	4	0, 1, 3, 6, 8.	N
8	6	4	2	0, 1, 2, 3, 4, 6.	N
13	6	2	6	1, 3, 4, 9, 10, 12.	Q
10	7	4	6	1, 2, 3, 5, 7, 8, 9.	D
13	8	4	8	1, 2, 3, 5, 8, 10, 11, 12.	C
19	9	4	0	1, 4, 5, 6, 7, 9, 11, 16, 17.	Q
17	9	4	8	0, 1, 2, 4, 8, 9, 13, 15, 16.	Q
14	11	8	6	0, 1, 2, 3, 4, 5, 7, 8, 9, 11, 13.	D
23	12	6	0	0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.	Q
21	12	6	12	1, 3, 4, 5, 6, 9, 12, 15, 16, 17, 18, 20.	N
16	12	8	12	1, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 15.	N
37	13	4	12	0, 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36.	C
19	13	8	12	0, 1, 2, 3, 5, 7, 8, 11, 12, 14, 16, 17, 18.	C
18	14	10	12	0, 1, 2, 3, 5, 6, 7, 9, 11, 12, 13, 15, 16, 17.	D
29	14	6	14	1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28.	Q
31	16	8	0	0, 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28.	Q
37	18	8	18	1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36.	Q

[a] Q = Quadratic residues.
D = Doubling (Construction 3.2).
N = None of the above.
C = Cubic residues.

$4 \leqslant k \leqslant 20$ satisfying Proposition 2.1. Most of these parameters were eliminated by the results on nonexistence in Section 5, together with Isbell's [2, Theorems 1.2 and 1.5]. For the remaining parameters, some corresponded to examples constructed in Section 3, viz. 17 trivial cases, 9 cases of quadratic residues, 3 cases of cubic residues, and 4 cases by Construction 3.2. By applying the method in Section 4 to the other cases, two more examples, viz. (9, 5, 2, 4) and (21, 12, 6, 12) were found, while all others except (8, 6, 4, 2), (16, 12, 8, 12), and (28, 19, 12, 18) were proved to be impossible. Those three cases were too big to be handled by the modulo p method. For the first two cases, perfect addition sets were constructed by hand, and the last case was eliminated by an argument:

Suppose a (28, 19, 12, 18)-perfect addition set A exists. The argument as used in the proof of Theorems 5.2 and 5.3 gives $\theta(x) \equiv 6x^3 + 3x^2 + 6x + 4 \bmod x^4 - 1$. Hence A contains (modulo 4) four 0's, six 1's, three 2's, and six 3's. The construction method in Section 4 gives $\theta(x) \equiv 3x^6 + 3x^5 + 3x^4 + 3x^3 + 3x^2 + 3x + 1 \bmod x^7 - 1$. Hence, A contains (modulo 7) one 0, three 1's, three 2's,..., and three 6's. Since $\mu = 18$, there are exactly eighteen elements a in A such that $-a$ $(\neq a)$ is also in A. Under such restrictions, there remains only three possible choices for A, none of which is a perfect addition set by direct checking.

REFERENCES

1. L.D. BAUMERT, "Cyclic Difference Sets," Lecture Notes in Mathematics, No. 182, Springer-Verlag, New York/Berlin, 1971.
2. J. R. ISBELL, Perfect addition sets, *Discrete Math.* **24** (1978), 13–18.
3. C. W. H. LAM, A generalization of cyclic difference sets, I. II. *J. Combin. Theory Ser. A* **19A** (1975), 51–65; 177–191.
4. C. W. H. LAM, Cyclotomy and addition sets, *J. Combin. Theory Ser. A* **22A** (1977), 43–60.
5. E. LEHMER, On the number of solution of $u^k + D = w^2 \pmod p$, *Pacific J. Math.* **5** (1955), 103–118.
6. T. STORER, "Cyclotomy and Difference Sets," Markham, Chicago, 1967.